Method of constructing hyperelliptic curves suitable for cryptographic purposes and cryptographic apparatus using such a method

In many cases, the secure exchange of information over public networks between senders and receivers requires the messages and documents due for exchange to be encrypted and therefore is in need of an authentication procedure for the senders and receivers.

An encrypting or cryptographic method that is encountered with particular frequency is what is termed "asymmetric" encryption, which is also known as the "public key" method. This method allows the receiver of a message to transmit a key over the public network to the sender, i.e. in such a way that it is, in principle, accessible to any third party. This key is the "public key". The sender then encrypts the message using this key. Where the power of the public key method lies is in that fact that a message that has been encrypted in this way cannot be decrypted again with a knowledge of the public key alone. Only the generator of the public key, i.e. the receiver, can decrypt the message encrypted with its public key. There are a number of variant types of asymmetric encryption of this kind. The most widely familiar example of an asymmetric method is undoubtedly the RSA method.

A subgroup of public key methods includes the step of exponentiating a very large natural number or integer modulo of another large natural number, the public key. The security of this group of methods is based on the impossibility in practice of calculating discrete logarithms in order to obtain the secret exponent in this way. Examples of methods of encryption and authentication based on the discrete logarithm problem are those known by the names Diffie-Hellman encryption, El-Gamal encryption, DSS signatures and Schnorr's method.

The finite Abelian group on which the discrete logarithm is based can be selected in various ways. One possible choice is the group of F_q-rational elements of the divisor class group of zero (0) degree of a hyperelliptic curve that is defined over a finite field F_q. For this group, which is also referred to as the F_q-rational point group of the Jacobi variety of the hyperelliptic curve, there exists a compact representation of the elements of the group and an efficient adding algorithm. Further details of the representation and use of this

group are discussed in, for example, N.Koblitz "Algebraic Aspects of Cryptology", Springer Verlag, 1998.

One problem with this choice is however the determination of a suitable hyperelliptic curve, To ensure that the discrete logarithm problem cannot be solved in practice, the divisor class group of this curve should include a very large prime factor, because the run time of algorithms to solve the logarithm problem depends on the square root of this prime factor. If the performance of today's computer systems is taken as a basis, the prime factor should be at least 2^{160} bits long. However, to ensure that the system is efficient, the parameters of the system, such as the keys for example, should not be too large.

Hyperelliptic curves that meet these conditions are curves whose zero degree divisor class group is of a prime or almost prime group order. To determine curves of this kind, it is, in principle, possible to select the coefficients of the curve randomly from the finite field F_p. If the resulting curve is non-singular, the number of elements of the divisor class group can then be determined. However, it has not so far been possible to find an algorithm that will determine this number, i.e. the order of the divisor class group, for a randomly selected hyperelliptic curve over a field having a large characteristic ($p > 2^{80}$ for genus 2 curves). In addition, only a fraction of hyperelliptic curves have a divisor class group of prime or almost prime order and because of this, even if there were such an algorithm, there would still be the problem of having to test a large number of curves before a curve that was secure in the sense defined above could be determined. These tests detract from the speed of the selection process.

It is therefore an object of the invention to define a method for the fast determination of secure hyperelliptic curves. It is further an object of the present invention to provide a cryptographic apparatus for carrying out such a fast determination of secure hyperelliptic curves.

For the purposes of the present invention, this object is achieved by constructing suitable hyperelliptic curves by using the method of complex multiplication. The inventive method generates, for cryptographic applications, suitable genus 2 hyperelliptic curves over finite fields having large characteristics.

A hyperelliptic curve of genus g over a field F_q (or F_p) having a characteristic not equal to 2 can be defined as a non-singular curve of the form

$y2 = f(x)$,

where f(x) is a normalized polynomial of degree 2g + 1.

The complex multiplication method, referred to below as the CM method, is known per se and has been used by Atkin for example to construct elliptic curves. For details of this known application of the CM theory, reference may made be made to: A.O.L Atkin, F. Morain, Elliptic curves and primality proving, Math. Comp. 61: 29-68, 1993. The known CM method makes it possible to determine, for a given imaginary quadratic order O and a prime number p, an elliptic curve E defined over F_p whose endomorphism ring is isomorphic to O. The complexity of the CM method and hence the computing work it involves is determined in this case by the class number h(O) and the discriminant of the order O. In dissertations by A.-M. Spallek [IEM, 1994, preprint no.18] and the present inventor A. Weng [IEM, 2002, preprint no.11], the application of the CM method was extended to the construction of hyperelliptic curves of genus 2 and class number 1 (Spallek) and to hyperelliptic curves of genus 2 and a class number of up to 10 and to special cases of hyperelliptic curves of genus 3 and above (Weng).

In particular, in the method according to the invention a representant system of all isomorphism classes of simple principally polarized Abelian varieties is determined. The counting of the isomorphism classes is simplified in this case because there is no need to check whether the fundamental unit is a relative norm of a unit in the CM field K.

Also the period matrices can be converted into equivalent Siegel-reduced matrices and a faster convergence of the theta nulls obtained in this way.

In a further preferred embodiment, the hyperelliptic curve over the field C of complex numbers is determined from six of ten theta nulls that are calculated.

Also, in a preferred variant of the method according to the invention, a plurality, and in particular more than a hundred or more than a thousand even, of possible CM fields are determined and the class polynomials belonging to the CM fields are calculated and the two are stored as a data set prior to use of the method for determining a secure hyperelliptic curve.

In a variant of the method according to the invention, the range of CM fields that are possible is reduced by a test. It can be ensured in this way that an exact prime number can be obtained for the group order.

In the method according to the invention, the prime number p on which the finite field F_p is based is selected in such a way that the minimum polynomial of the CM field K over F_p decomposes into four different linear factors.

In another variant, the finite field F_q on which the curve is based is not prime.

A cryptographic apparatus making use of a method as described beforehand can advantageously be used for encrypting and decrypting of messages for the secure exchange of information over public networks between senders and receivers. With such a cryptographic apparatus, messages and documents due for exchange can be encrypted fast and easily in an authentication procedure for the senders and receivers.

These and other aspects of the invention are apparent from and will be elucidated with reference to the embodiments described hereinafter.

In the drawings:

Fig. 1 shows a first sub-step according to the invention for determining a CM field and the associated class polynomials.

Fig. 2 shows a second sub-step according to the invention for determining a curve suitable for cryptographic purposes.

In what follows, steps of the method according to the invention will be described in detail. The method includes two sub-steps. The first sub-step relates to the determination of a CM field K, of a prime number p suitable for defining the field F_p, and of a suitable group order n.

A suitable CM field K is first determined by a total imaginary quadratic expansion of a totally real number field K_O having a class number $h_{KO} = 1$. A CM field of this kind may for example be given by the set $K = Q(i(a + bd)^{1/2})^{1/2})$, where a, b and d are integers.

The prime number p is selected in such a way that the following three conditions are met:

1. There is a number w in O_K such that $w\underline{w} = p$, where O_K is the maximum order of K and $\underline{w}$ is the conjugate complex element of w (here and in what follows, the underlining indicates the conjugate complex element of the item underlined).

2. Either $n_1 = \Pi(1 - w_i)$ or $N_2 = \Pi (1 + w_i)$ is almost prime, where the product Π covers all the conjugates w_i of w in K.

3. One of the orders n_i (i = 1,2) is of the form kq, where k is a small number and q is a prime number that meets the condition that the order of p in F_q is high.

The selection of p can be simplified in this case by selecting a random number η from O_K and checking whether the conjugate complex element of the product $\eta\bar{\eta}$ is a prime number. If it is, n_1 or n_2 can be checked for compliance with condition 2. The number η should be selected in this case in such a way that it is ensured that its relative norm is a member of the set Z of integers.

Alternatively, a random number p can be selected from Z and the minimum polynomials in Z[x] can be determined for all the solutions of the absolute norm equation $N_{K/Q}(w) = p^2$. From these polynomials, the ones that are irreducible and have zero points of an absolute value $p^{1/2}$ are selected. These minimum polynomials are then analyzed at the point x = 1. This gives a set S of possible group orders n_i. This set has at most four different members. These values n_i can then be tested for compliance with conditions 1 and 2 above.

For the subsequent second sub-step, it can be assumed that a CM field K, a prime number p and a group order n have been determined that meet conditions 1-3 in the first sub-step. In this second sub-step, a hyperelliptic curve over F_p is constructed that has a divisor class group of order n.

In so doing, advantage is taken of the fact that, in the case of hyperelliptic curves of genus 2, the Jacobi varieties of these curves are exactly the principally polarized Abelian varieties of dimension 2. Also, it is possible, using known methods, to find a representant system for all isomorphism classes of simple principally polarized Abelian varieties of the field C of complex numbers that have complex multiplication by O_K. It is also known in principle for a period matrix Ω of these varieties to be determined from the set H_2, where $H_2 = \{M \text{ from } Gl_2(C), M^t = M, \text{ with Im M being positively definite}\}$ is the Siegel upper half-plane of dimension 2. The matrix is thus symmetrical and has a positively defined imaginary part.

Let the following be taken as an example:

$K_0 = Q(6^{1/2})$ where $O_{K0} = Z + \omega Z$, $\omega = 6^{1/2}$

$K = Q(i(3 + 6^{1/2})^{1/2})$

p = 139703394307053467381009 41, and

n = 1951703838090595750309289207140118513549719642383 76.

η is taken as equal to $i(3 +)^{1/2})$. The fundamental unit ϵ_0 of $Q(6^{1/2})$ has a positive norm in this case. A representant system of the ideal class group that is relatively complete with respect to the real quadratic subfield O_{K0} can be represented as:

$$I_K = \{A_1 = O_K = O_{K0} + \eta O_{K0},\ A_2 = (1 - 6^{1/2})\ O_{K0} + (-1 + \eta)\ O_{K0}\}.$$

From the general representation of A1 and A2:

$Ai = \alpha O_{K0} + \beta O_{K0}$,

$\tau_i = \alpha/\beta$ is calculated, where, taking the above example,

$\tau_1 = 0.42837299059613220 11i$

$\tau_2 = 0.2247448713915890490 + 0.52464762327529031 78i$.

An embedment σ of K in the field of complex numbers C is given by

$\sigma\,(i\,(3 + 2^{1/2})^{1/2}) = -i\,(3 - 2^{1/2})^{1/2}$ and

ρ as the conjugate complex element thereto. A representant system of all the isomorphism classes of simple principally polarized Abelian varieties that have multiplication by O_K is then given by the set of tuples

$$\{(\tau_1, \tau_1^{\sigma}), (\epsilon_0 \tau_1, (\epsilon_0 \tau_1)^{\sigma}), (\tau_1, \tau_1^{\rho\sigma}), (\epsilon_0 \tau_1, (\epsilon_0 \tau_1)^{\rho\sigma})\}.$$

The associated period matrix for a tuple (s_1, s_2) is

$$\Omega_{s1,s2} = \frac{1}{\omega - \omega^{\sigma}} \begin{pmatrix} \omega^2 s_1 - \omega^{\sigma 2} s_2 & \omega s_1 - \omega^{\sigma} s_2 \\ \omega s_1 - \omega^{\sigma} s_2 & s_1 - s_2 \end{pmatrix}$$

By the following procedure, a count is obtained of the isomorphism classes, if the field $K = Q(i(a + bd^{1/2})^{1/2})$ is a CM field, $\epsilon 0$ is the fundamental unit, σ is the conjugation

$\sigma\,(i(a + bd^{1/2})^{1/2}) = -i(a - bd^{1/2})^{1/2}$

and ρ is the complex conjugation. For a representant $A_i = \alpha_i O_{K0} + \beta_i O_{K0}$, $\tau_i = \alpha_i/\beta_i$ is obtained where $\mathrm{Im}(\tau_i) > 0$. With $\{\tau_1, \ldots\ldots, \tau_k \ldots\ldots, \tau_{hk}\}$ and $k \leq h$ as a class group, it is the case that $\mathrm{Im}\ \tau_i^{\sigma} > 0$ for $i \leq k$ and $\mathrm{Im}\ \tau_i^{\sigma} < 0$ for $i > k$. The following rules allow a suitable set S of simple principally polarized Abelian varieties that are complexly multipliable with O_K to be obtained:

If K is Galoisian, then $S := \{(\tau_i, \tau_i^{\sigma}),\ 1 \leq i \leq h\}$.

If K is non-normal and if $N(\epsilon_0) = 1$ then $k := h/2$;

$S := \{(\tau_i, \tau_i^{\sigma}), (\epsilon_0 \tau_i, (\epsilon_0 \tau_i)^{\sigma}),\ 1 \leq i \leq k\} \cup \{(\tau_i, \tau_i^{\rho\sigma}), (\epsilon_0 \tau_i, (\epsilon_0 \tau_i)^{\rho\sigma}),\ k + 1 \leq i \leq 2k\}$,

and if K is non-normal but $N(\epsilon_0) = -1$ the definition obtained is as follows:

$S := \{(\tau_i, \tau_i^{\sigma}), (\epsilon_0 \tau_i, (\epsilon_0 \tau_i)^{\rho\sigma}),\ 1 \leq i \leq h\}$.

For each matrix of the period matrix Ω_i determined above where $i = 1, \ldots, 4$, the absolute invariants $j_k^{(i)}$ are then calculated with $k = 1, 2, 3$. For this purpose, the even theta-nulls are first calculated for each matrix Ω_i and with the help of the theta-null, that curve over C is determined whose Jacobi variety corresponds to the period matrix Ω. The class polynomials of the curve are calculated from the absolute invariants.

The even theta-nulls of a period matrix Ωi are given by

$$\theta\begin{bmatrix}\delta\\ \varepsilon\end{bmatrix}(\Omega_i)=\sum_{n\ from Z^g} exp\left(\pi i\left((n+1/2\delta)^t\,\Omega_i\,(n+1/2\delta)+2(n+1/2\delta)(z+1/2\varepsilon)^t\right)\right),$$

with δ, ϵ from the set $\{0,1\}^g$, $\delta^t\epsilon = 0 \bmod 2$.

For genus 2 curves, this function gives exactly ten theta-nulls. The quality of the approximation should be selected such that the approximation of the class polynomials calculated subsequently is adequate for a smooth number n to be in Z[1/n][X]. In the example described, seventy decimal places is enough.

The convergence of the equation with the theta-nulls can be improved if Siegel-reduced matrices Ω' are inserted in the function rather than the matrices Ω_i from H_2. A matrix $\Omega' = X + iY$ from H_2 where $X = (x_{kl})$ with subscripts $k,l = \{1,2\}$ is Siegel-reduced if the following are true:

1. $1/2 \leq x_{kl} \leq -1/2$
2. Y is Minkowski-reduced
3. $|\det (CZ + D)| \geq 1$ for all $\begin{pmatrix}A & B\\ C & D\end{pmatrix} \in Sp(4,Z)$.

By means of the theta-nulls, a model of the curve over C that is being looked for can be determined. The Rosenhain model is a model of this kind

$$y2 = x(x - 1)\,\Pi\,(x - \lambda_i),$$

where the subscript i extends from 1 to 2g-1, i.e. for curves of genera 2 to 3. The Rosenhain model allows the λ_i values to be calculated from the theta-nulls. The following are the case in the example below:

$\lambda_1 = 3.7761476679542305243215 + 1.0919141042403378864850i$

$\lambda_2 = \underline{\lambda_1}$

$\lambda_3 = -0.5826628324044744213034.$

From the 10 even theta-nulls, the so-called absolute Igusa invariants j_1, j_2, j_3 are also obtained as known functions.

Both the λ_i's of the Rosenhain model and the Igusa invariants can however also be determined simply from six theta-nulls:

$$\alpha_1=\theta\begin{bmatrix}(00)\\ (10)\end{bmatrix}\quad \alpha_2=\theta\begin{bmatrix}(01)\\ (10)\end{bmatrix}\quad \alpha_3=\theta\begin{bmatrix}(11)\\ (10)\end{bmatrix}$$

$$\alpha_4 = \theta\begin{bmatrix}(00)\\(10)\end{bmatrix} \quad \alpha_5 = \theta\begin{bmatrix}(01)\\(10)\end{bmatrix} \quad \alpha_6 = \theta\begin{bmatrix}(11)\\(10)\end{bmatrix}$$

The λ_i's of the model

$f(x) = x(x-1)(x - \lambda_3)(x - \lambda_3)(x - \lambda_5)$ are given by:

$$\lambda_3 = \alpha_1^2\alpha_2^2(\alpha_3^2\alpha_4^2)^{-1}$$
$$\lambda_3 = \alpha_5^2\alpha_2^2(\alpha_3^2\alpha_6^2)^{-1}$$
$$\lambda_3 = \alpha_5^2\alpha_1^2(\alpha_4^2\alpha_6^2)^{-1}$$

and the (non-absolute) Igusa invariants are defined by

$$I_2 = -120A', \; I_4 = -720(A')^2 + 6750\,B',$$
$$I_6 = 8640(A')^3 - 108000A'B' + 202500C' ..$$

where

$$A' = (f, f)_6, \; B' = (i, i)_4., \; C' = (i, \Delta)_6 \text{ and}$$
$$i = (f, f)_4, \; \Delta = (i, if)_2$$

where the term $(gh)_k$ represents the overlaying of two binary forms g and h of degrees n and m, of the form

$$(gh)_k = \frac{(m-k)!(n-k)!}{m!\,n!}\left(\frac{\delta g}{\delta x}\frac{\delta h}{\delta z} - \frac{\delta g}{\delta z}\frac{\delta h}{\delta x}\right).$$

The absolute invariants can then be obtained from the Igusa invariants:

$j_1 = I_2 I_4^2 / \Delta, \; j_2 = I_2^3 I_4 / \Delta, \; j_3 = I_4 I_6 / \Delta.$

The calculation of the Igusa invariants may be further speeded up by sorting the group I_K of ideal classes into pairs of ideal classes and their inverses. Because it is true in the case of the field K_0 of class number 1 that the inverse ideal classes are equal to the conjugate complex ideal classes, only one simple principally polarized Abelian variety need be calculated for each pair of conjugate complex ideal classes that is found:

If (τ_1, τ_1^{ψ}) is the principally polarized Abelian variety belonging to the ideal A_i and the CM type (K, ψ), then $(-\underline{\tau}_1, -\underline{\tau}_1^{\psi})$ is the principally polarized Abelian variety of the same CM type, belonging to $\underline{A}_i$. If in addition j_i is the Igusa invariant of (τ_i, τ_i^{ψ}), then the corresponding Igusa invariant of $(-\underline{\tau}_i, -\underline{\tau}_i^{\psi})$ is equal to $\underline{j}_i$. Hence, only one Igusa invariant needs to be determined for each pair of inverses of conjugate complex ideal classes. Consequently, the amount of computing work required for this step is almost halved.

The class polynomials H_k can be represented as functions of the Igusa invariants j_k, $k = 1, \ldots, 3$:

$H_k(X) := \Pi (X - j_k^{(i)})$, where $i = 1, \ldots, 4$).

The polynomials are members of the corpus of rational polynomials Q[x]. By applying the method of infinite continued fractions followed by multiplication, $K_k(X)$ can be converted into an integer polynomial $H_k(X)^{\#}$. What is obtained in the example for

$H_1(X) = \Pi (X - j_1^{(i)})$ is

$$- 46989351758.431801106481797\ X^3$$
$$- 45970146813147129.294447100607881\ X^2$$
$$+ 109244593815490693040 09.28898299296496140\ X$$
$$+ 626622028994536625011952 73.54688887371081210299.$$

If the accuracy is selected to be sufficiently high, the least common multiple of the denominators of the coefficients is found with the continued fraction algorithm. In the present example this is 11^4. This gives the integer polynomial:

$$H_k(X)^{\#} = 14641\ X^4 - 687971099095200\ X^3 - 673048919491287120000\ X^2$$
$$- 15994500980525992368000000 0\ X$$
$$+ 91743731265090107268000000 0000.$$

The class polynomials of the form $H_k(X)$ over Q[x] and of the form $H_k(X)^{\#}$ over the field of integer polynomials Z[x] depend only on the CM field K that is selected. The basic prime number field F_p for the hyperelliptic curve may however still vary even after the CM field K has been selected. Ii is therefore advantageous for a large number, hundreds or thousands in practice, of suitable CM fields and the associated class polynomials to be calculated in advance and stored in some suitable manner. If after this step it is necessary for a hyperelliptic curve to be generated for the application of encryption, recourse may be had to a randomly selected CM field, or in other words to randomly selected class polynomials, from the file held in store, and a suitable prime number p and group order n may be determined by the criteria listed in the first sub-step. After that, the following steps may be performed immediately to determine the hyperelliptic curve over F_p without the class polynomials having to be re-determined.

For the implementation of a cryptographic protocol, it may also be advantageous for the operation to be confined to group orders that are exactly prime.

For this purpose, it is proposed that the selection of the CM fields be limited and that the only CM fields K used be ones for which the minimum polynomial K/Q modulo 2 has two different factors or is irreducible.

So, for the following steps for calculating the hyperelliptic curve over F_p, it is assumed that the CM field K has been selected and the class polynomials $H_k(X)^{\#}$ have either been calculated by performing the steps described above or have been taken from a file that was calculated in advance.

The next step is to calculate the curve. For this purpose, the following steps are performed for each tripel (a_1, a_2, a_3) from $(F_p)^3$ with $H_k(X)^{\#}(ak) = 0 \bmod p$:

Set $j_1 := a_1$, $j_2 := a_2$ and $j_3 := a_3$. Then calculate the Mestre invariants A_{ij} and H_{ijk} from j_i. Under the known Mestre procedure for finite fields, as described for example in J.-F. Mestre, "Constructions des courbes de genre 2 à partir de leur modules", Progr. Math. Birkhäuser, 94: 313-344, 1991, the Mestre invariants are coefficients of a quadric of the form

$$\Sigma A_{ij} x_i x_j$$

and of a cubic of the form

$\Sigma H_{ijk} x_i x_j x_k$, where the summing extends through subscripts i, j, k from 1 to 3.

By setting parameters for the quadric by taking polynomials $f_1(t)$, $f_2(t)$, $f_3(t)$ and inserting them in the cubic

$$\Sigma H_{ijk} f_i(t), f_j(t), f_k(t)$$

a model

$$y^2 = f(t)$$

of the hyperelliptic curve over F_p can be obtained. The degree of the polynomial f(t) (generally 6) can then by reduced by one to 5 by projective transformation if f(t) has a zero point in F_p. Then check whether the divisor class group of the curve is of order n by selecting a random divisor D and forming the product nD.

The resulting curve in the case of the example given is

$$y^2 = x^5 + 44645056158389978352246 00 x^4 + 11942994115339229240469614 x^3 + 11085840639937493508880 07 x^2 + 11457344736666435422023499 x + 29010666429869784066756 71.$$

and is defined over the field F_p where

p = 139703394307053467381009 41 and

n = 19517038380905957503092892071401185135497196423837 6

are equal to the above mentioned values. The value of n is 152 times a prime number.

The Mestre algorithm can be speeded up selecting a suitable prime number p. Prerequisites for this are that the CM field K is non-normal and p is a prime number belonging to the set of integers Z that is completely decomposed in K or, which is equivalent to this, the minimum polynomial of K in F_p can be decomposed into four different linear factors. Under these conditions, the number of linear factors modulo p for each class polynomial is halved, provided the above equation $w\underline{w} = p$ has, except for the sign and the conjugate complex element, only one solution w from the set O_K. This halving of the linear factors speeds up the application of the Mestre algorithm by a factor of 8.

To allow this advantage to be exploited, a check is made to see whether a primary number p determined in the first sub-step above decomposes the minimum polynomial of K in F_p into four different linear factors. This can be done by direct calculation. If however, as described above, p was selected by analysis at the point x = 1 of minimum polynomials in Z[x] that are irreducible and have zero points at the absolute value $p^{(1/2)}$, the prime numbers found are already presorted. After this, the prime numbers can be confined to ones that permit only two different group orders.

If the CM field is cyclic and the exponent of the ideal class group is larger than 2, then the prime numbers that are advantageous in this sense are of positive density. In particular there are an infinite number of such prime numbers.

The method described for generating a hyperelliptic curve suitable for cryptographic purposes may be expanded to cover non-prime finite fields F_q. The number $q := p^f$ is defined as a power of a primary number p in this case. The exponent f is a natural number and is referred to as a degree of expansion. It may also be assumed that the curve cannot be defined over a subfield of F_q.

In the event of the CM field K being Galoisian, p should be selected such that

$p = A\underline{A}$ in K/K_0.

If f is selected to be a minimum under the condition that

$A^f = (w)$, w being an element from O_K,

is a main ideal, then there is a square root of the class polynomials over F_q. Hyperelliptic curves over F_q can be constructed as detailed above from these roots by means of the Mestre algorithm. The order of these curves is given by

$$n = \Pi (1 - w_i) \text{ or } \Pi (1 + w_i)$$

where the subscript $i = 1, \ldots, 4$ and w_i is the conjugate complex element of w.

In the event of the CM field being non-Galoisian and non-normal, the prime number p should be selected such that the prime ideal (p) decomposes into three ideals:

$(p) = p_1p_2p_2$.

There is then an ideal A, which means that

$A = p_1p_2^2$

and f is again selected to be a minimum with

$A^f = (w)$, with w being an element from O_K.

Under these conditions, hyperelliptic curves over the non-prime finite fields F_q, where $q = p^{2f}$, can be constructed as detailed above by means of the Mestre algorithm. The group order can be calculated as in the case of a Galoisian field K.

As an example, a curve will be constructed over a field of the degree of expansion $f = 2$ $h_k = 10$, starting from a CM field K having a class number $h_K = 5$. What will be used as a prime number is $p = 911$, whose ideal (p) over the field K decomposes into three prime ideals. For ideal $A = p_1p_2^2$, $f = 5$ is the smallest exponent. The main ideal is therefore A^f.

The elements in F_q with $q = 911^{10}$ can be stated by polynomials of degree 9. The modulo p irreducible class polynomials are

$H_1(X) = 701X^{10} + 401X^9 + 322X^8 + 712X^7 + 125X^6 + 774X^5 + 513X^4 + 869X^3 + 474X^2 + 49X + 680 \bmod p$

$H_2(X) = 186X^{10} + 895X^9 + 453X^8 + 86X^7 + 180X^6 + 47X^5 + 811X^4 + 339X^3 + 887X^2 + 296X + 371 \bmod p$

$H_3(X) = 75X^{10} + 280X^9 + 616X^8 + 737X^7 + 511X^6 + 179X^5 + 623X^4 + 533X^3 + 616X^2 + 697X + 700 \bmod p$

Two possible group orders are obtained:

$n_1 = 155012792308846128138632814006095268154658315370266774539376$

$n_2 = 155012792308846046374979954330693046736810307187589966188400$

The associated curve $y^2 = f(x)$ is

$f(x) = x5 + [9\ 703\ 722\ 261\ 507\ 119\ 322\ 684\ 741]\ x^4$

$+ [715\ 508\ 396\ 153\ 661\ 164\ 513\ 167\ 892\ 156]\ x^3$

$+ [548\ 810\ 311\ 54\ 483\ 636\ 130\ 899\ 845\ 101]\ x^2$

$+ [550\ 294\ 663\ 157\ 288\ 697\ 710\ 60\ 475\ 608]\ x$

$+ [301\ 385\ 355\ 533\ 347\ 763\ 659\ 163\ 720\ 665],$

use having been made of the abbreviating notation

$a_0 + a_1z + a_2z^2 + a_3z^3 + \ldots + a_8z^8 + a_9z^9 = [a_0\ a_1\ a_2\ a_3\ \ldots\ a_8\ a_9]$.

The group order is $n_2 = 400r$, where r is a prime number having 57 decimal places.